RI Spotlight

April 2024

Embedding cyber security

Triton

Triton at a glance[1]

Founded in
1997

Professionals accross
11 offices

Integrated operating & specialist teams

€19 billion
Raised since inception

200+
Institutional investors

100+
Investment advisory professional across three investment strategies

60+
Operational and functional specialists supporting value creation through the investment life cycle

Portfolio companies

100+
Investments since inception

600+
Add-on acquisitions completed

€18 billion+
Combined portfolio revenues

100,000+
Full-time employees at portfolio companies

Core Triton sectors

- Business Services
- Industrial Tech
- Healthcare

Strategies

Capital raised

€15.5bn
Mid-Market PE

€1.3bn
Smaller Mid-Market PE

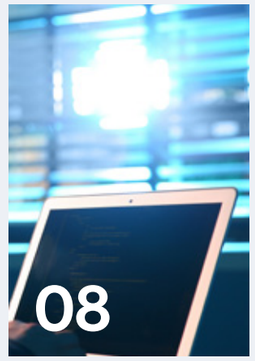
€2.1bn
Credit

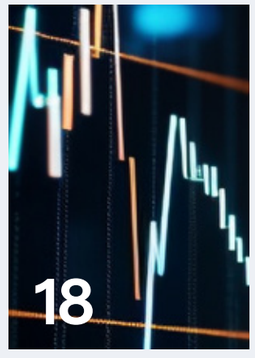
[1] As of December, 2023

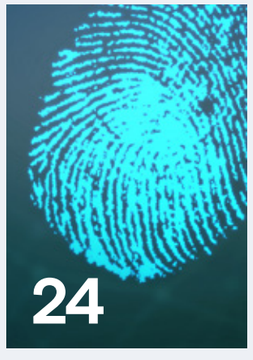
Triton and its portfolio companies (PCs) benefit from West Park and the services provided by it. Since its formation in 2007, West Park has become a core part of Triton's "Building Better Businesses" strategy and approach. West Park is able to provide a range of value-adding services to support the investment process and portfolio companies that would otherwise be provided by third parties.

Embedding cyber security

Contents







Welcome from our Managing Partners

Peder Prahl
CEO & Firm Managing Partner

Martin Huth
Firm Managing Partner

Companies in all sectors have long, if not always, had to face and address crime. Damage to property; theft from premises; corruption; threats to employees; illegally substandard and dangerous goods and services from third party subcontractors – the list of criminal activities posing material risks to companies is lengthy. Each category of risk requires a specific system response – policies, protocols, trained staff, investment in equipment. Viewed in this way, cybercrime may be a new crime risk, but otherwise, is no different.

Cybercrime is a broad category of emergent risk to businesses, public authorities and individuals. It includes criminal activities that are carried out using computer networks, digital devices, and the internet. Though a relatively recent phenomenon, cybercrime has grown incredibly fast and now poses a major threat to companies around the world.

The global response is also now developing rapidly. Computing giant Microsoft reported that, in 2022 alone, it blocked 70 billion email and identity threat attacks while also blocking 2.75 million site registrations planned for use in global cybercrime.

Meanwhile, law enforcement agencies from around the world are collaborating to investigate and address risks from what is essentially a borderless category of crime, and are targeting criminal gangs.

In this report, we explore how digitalisation of society and economic activity has led to the evolution of cybercrime. We then examine the steps being taken to counteract it and provide safeguards, before considering what Triton's Digital and ESG teams are doing to mitigate associated risks. This includes our Triton Cyber 360 assessment, as well as the steps our portfolio companies are taking.

Triton Embedding cyber security - April 2024

"Criminals from every corner of the globe attack our digital systems on a near constant basis. They strike targets large and small - from corporate networks to personal smart phones. No one - and no device - is immune from the threat."

US Federal Bureau of Investigation[1]

[1] Internet Crime Complaint Center(IC3) | Home Page
[2] Global cybercrime estimated cost 2028 | Statista

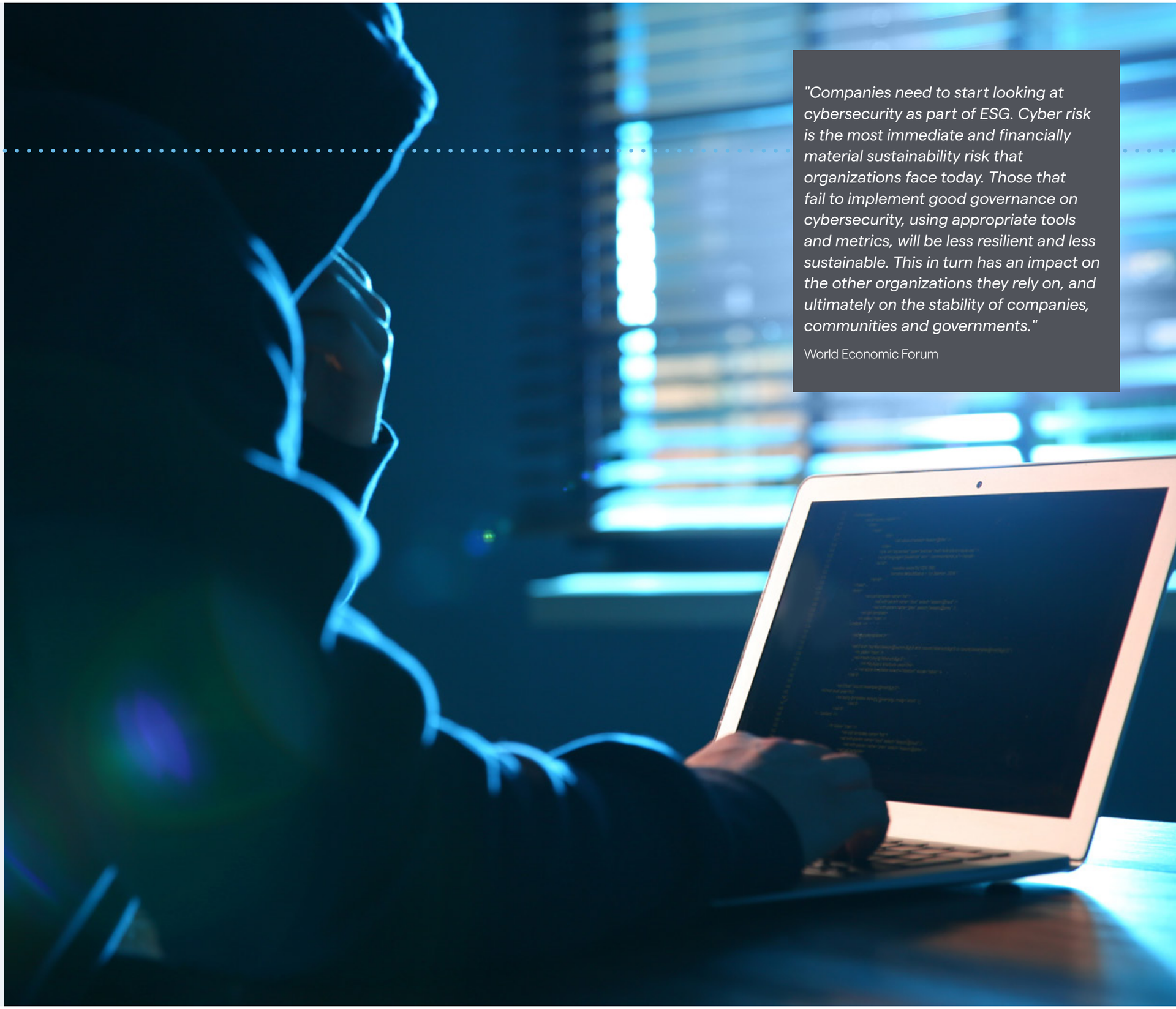
The rise of cybercrime

Risks and opportunities with digital tech

Digital technology has brought huge opportunities – from computer processing power, through to satellite communications, the internet and artificial intelligence.

The downside, however, is that it also increasingly harbours risks, and of truly consequential levels. Cybercrime is now a global threat, ever-diversifying and hugely lucrative to the criminal gangs involved. Some estimates for the combined losses from cybercrime run at over a trillion dollars now, completely dwarfing the losses from traditional physical bank robberies.

Triton
Embedding cyber security - April 2024



"Companies need to start looking at cybersecurity as part of ESG. Cyber risk is the most immediate and financially material sustainability risk that organizations face today. Those that fail to implement good governance on cybersecurity, using appropriate tools and metrics, will be less resilient and less sustainable. This in turn has an impact on the other organizations they rely on, and ultimately on the stability of companies, communities and governments."

World Economic Forum

Cyber crime categories

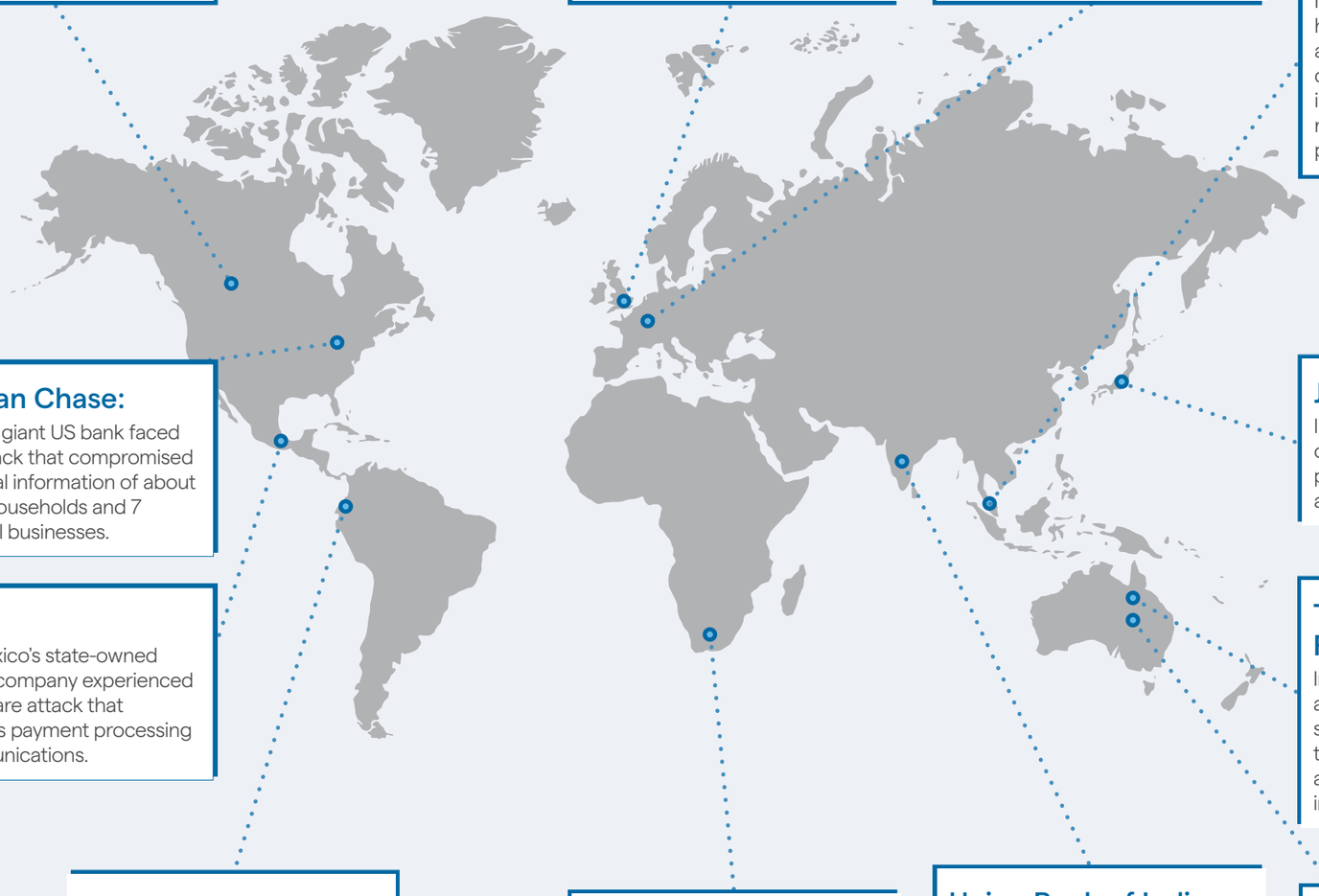
Cybercrime is a broad category. A 2023 survey by Allianz Risk Barometer found that companies were most concerned about data breaches, followed by the increase in ransom attacks, failures in digital supply chains, and malware attacks.

A global crime category

Anders Thulin
Head of Digital & Technology at Trinton Partners

"Cybercrime is a massive concern. The speed with which it has climbed the list of material challenges which businesses face has been astonishing – the global response has been quick to follow, but if anything, has struggled to keep up. That is evident in the trillions of dollars now lost each year to criminals operating in this space.

At Triton, we need to ensure that our portfolio companies are adequately equipped to fend off cyber attacks, and also to respond quickly, with efficacy, if and when they do fall victim. Triton's Cyber 360 assessment is a key part of our Triton Digital and IT 360 strategies."



University of Calgary:
In 2016, the University fell victim to a ransomware attack that disrupted its computer systems and resulted in a payment to the attackers to restore access to the encrypted data.

British Airways:
In 2018, the UK airline suffered a data breach that affected around 500,000 customers, involving the theft of personal and financial information, including names, addresses and credit card details.

Deutsche Telekom:
In 2016, the TelCo experienced a massive cyber attack that affected over 900,000 of its customers, disrupting internet services and causing network outages.

SingHealth:
In 2018, Singapore's largest healthcare group experienced a major data breach that compromised the personal information, including medical records, of around 1.5 million patients.

JPMorgan Chase:
In 2014, the giant US bank faced a cyber attack that compromised the personal information of about 76 million households and 7 million small businesses.

Pemex:
In 2019, Mexico's state-owned petroleum company experienced a ransomware attack that impacted its payment processing and communications.

Japan Pension Service:
In 2015, a data breach affected over 1.25 million users, with leaked personal data, including names and pension numbers.

Toll Group Ransomware Attack:
In 2020, the Australian logistics and transportation company suffered a ransomware attack that disrupted its operations and led to temporary service interruptions.

Banco del Austro:
In 2015, the Ecuadorian bank experienced a cyber heist in which hackers stole approximately $12 million by using malware to manipulate SWIFT transactions.

City of Johannesburg:
In 2019, the largest city in South Africa experienced a ransomware attack that affected its IT systems and led to the shutdown of many municipal services.

Union Bank of India:
In 2016, the bank reported a significant cybersecurity incident in which hackers conducted unauthorised transactions through the SWIFT messaging system.

Australian finance industry:
In 2020, multiple organizations were targeted by a group using a "copy-paste" technique to deploy malware.

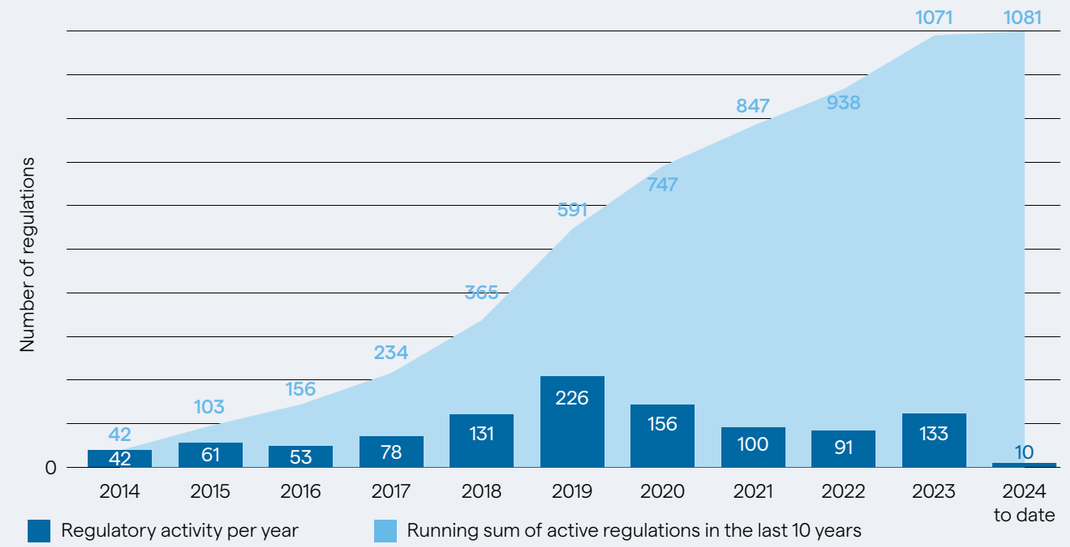
The growing global initiatives and regulations around cyber security

Over the last ten years, the number of consumer privacy and data protection regulations has grown. The chart on the right shows a total of 1081 regulations being passed across Europe over this period.

Alongside regulation, consumer privacy and data protection initiatives have also increased substantially within the last few years.

The list of initiatives includes the Sustainability Accounting Standards Board (SASB), Global Reporting Initiative (GRI), European Financial Reporting Advisory Group (EFRAG), European Data Protection Board, Task Force on Climate-related Financial Disclosures (TCFD), European commission, and the Competition and Markets Authority (CMA).

European privacy and data regulations



Source: Datamaran

Globally, multiple organisations are working together to combat cybercrime. Law enforcement agencies have signed mutual legal assistance treaties and other agreements to share information, gather evidence, and coordinate investigations into cybercrime cases that have cross-border implications.

Cross-border entities such as INTERPOL and EUROPOL facilitate international cooperation among police forces and law enforcement agencies globally and within regions.

International conventions and treaties, such as the Budapest Convention on Cybercrime, provide a framework for countries to cooperate in investigating and prosecuting cybercrime offenses.

Countries participate in information sharing networks, such as the US Department of Homeland Security's Automated Indicator Sharing programme, to exchange cyber threat intelligence in real time. In many instances, developed countries provide assistance and capacity-building programmes to help less developed nations enhance their cybersecurity capabilities and combat cybercrime effectively.

Public-private partnerships are also important – with governments and companies working together to share threat intelligence, best practices and resources to strengthen cybersecurity defences.

Objectives of the UN Global Programme on cybercrime

- Increased institutional efficiency and effectiveness in the prevention, disruption, investigation, prosecution and adjudication of cybercrime, in line with human-rights principles.
- Strengthened national and international communication and cooperation between government, law enforcement and the private sector to enhance prevention, disruption and investigation of cybercrime.
- Increased knowledge and sensitise society to reduce cybercrime risks.
- Adoption of effective regulatory frameworks leading to a sustainable and long-term response to counter cybercrime according to international standards.

Source: United Nations Office on Drugs and Crime

$4.45 million

Average cost to businesses of a data breach in 2023, an all-time high (IBM)

How Triton supports its portfolio

> The mid-market segment in which Triton invests is often described as the 'cybercrime sweet spot'[3]. One reason for this is the perception amongst cyber-criminals that, while at large cap companies it can be difficult to find anybody able to make payments to address threats posed, at smaller and medium sized companies this may be more possible.

Cyber security is therefore a core focus at Triton. The ESG team collaborates with the Digital team to ensure Portfolio companies (PCs) reduce the risk of cyber attacks as much as possible. All workstreams related to cyber – from mitigation to prevention – are carried out with full board oversight. On an annual basis, the Digital and ESG teams assess each PC via a 50-point questionnaire and a workshop to understand its cyber risk level. The scope of the Triton Cyber 360 assessment includes all entities within the PC ownership, across geographies, business units and departments.

Where risks are identified, a roadmap is developed based on the assessment to address and mitigate these.

The objectives of carrying out the cyber risk assessments are to introduce a collaborative approach to increase cyber security maturity, protect and enhance the value of the business and essentially to prevent business disruption.

[3] For context on the risks faced by SMEs, see research including: (1) Barracuda, 2022 – 'Spear Phishing: Top Threats and Trends' (2) Accenture, 2022 – 'Cost of Cybercrime' and (3) Hiscox, 2022 – 'Cyber Readiness Report

Triton Embedding cyber security - April 2024

How Triton supports its portfolio (cont)

The cyber risk assessment consists of the following approach:

Assessment → **Mitigation plan** → **Roadmap** → **Monitoring**

Partnership & Collaboration → **1-2 days work for PC Team**

Receive link to questionnaire

Kick-off call with PC stakeholders

Preparation

Entity scope

Documentation guidance

Workshop

Guided assessment

CISO/CTO/ CIO/Head of Information Security

Report production

Scoring

Benchmark

Recommendations

Follow-up meeting

Refine answers

Discuss recommendations

Agree final report

Optional mitigation planning

Final report delivered

Agree monitoring schedule

ISF Membership Session

Distribution to Deal Captain, Digital Sponsor & PC Stakeholders

Within the Stewardship programme, the ESG team asks PCs on an annual and periodic basis:

- to give updates on any cyber security breaches and mitigation and monitoring efforts
- whether PCs have in place a cyber security policy and if it is up to date
- percentage of employees trained in cyber security
- that PCs hold cyber security insurance

In addition to the above, Triton holds quarterly sessions with PCs to inform them on cyber updates and best practices. Policy templates are also updated on a regular basis and made available for PCs to use.

We refined our processes in H2 2023, and have moved to cloud services and SAS, bringing less direct exposure.

Triton also assists its PCs via an annual cyber security day, and through assistance with obtaining appropriate cyber insurance, to enable expertise sharing across our portfolio and supply chain.

"As the threats from cyber attacks are becoming increasingly sophisticated and frequent, being covered by cyber security insurance has never been as important as it is in this point in time."

Graeme Ardus
Head of ESG

From the portfolio perspective

Mitigating and building resilience

HiQ is a leading Nordic digital transformation company with a reputation for having amongst the strongest industrial and technology expertise in its market. Digital services, systems and products are at the core of HiQ's business offer, spanning from initial business development and digital innovation of new services, business models and experience, all the way to implementation and marketing of these services. Triton invested in HiQ in 2020.

Swiss IT Security Group is a leading independent cyber security service platform in the DACH and Benelux region. The company offers cyber security solutions along the customer journey, offering cybersecurity consulting and engineering, hard- and software sales, managed security services, SLAs and product maintenance for own and third-party products. Triton invested in Swiss IT Security in 2021.

HiQ has supported several Triton portfolio companies in improving their cyber security and data governance. HiQ is also supporting in managing data breaches and building resilience.

Swiss IT Security and HiQ are supporting Triton in managing the cyber assessments performed for each portfolio company, and offering mitigation plans if any gaps are identified that need addressing.

Interview

with Triton Head of Technology

Lyndon Arnold
Head of Technology at Triton Partners

Ashim Paun
Head of Sustainable Investing at Triton Partners

AP It seems we hear a lot about cybercrime these days. Do the risks justify this amount of noise?

LA The risks relating to cybercrime are significant and multifaceted. A ransomware incident can inflict severe consequences on businesses, causing disruption by encrypting critical data that can cripple operations for extended periods. The associated downtime results in financial losses coupled with the direct costs incurred in the crisis recovery. Moreover, the incident can cause reputational damage, eroding trust among clients, partners, and stakeholders, leading to long-term damage. Finally, regulators globally have continued to increase fines for data breaches for firms without adequate security measures in place to protect digital assets.

AP Are there specific categories of cybercrime which pose greater risks to our portfolio companies?

LA Triton portfolio companies are often growing through acquisition. In this fast moving and complex environment, businesses need to be aware of the risk of the so called "CEO Fraud". This is where sophisticated bad actors try to infiltrate communications systems and impersonate senior executives, advisors or lawyers in order to elicit payments from portfolio company finance staff.

AP What can companies do to mitigate the risks?

LA Companies can enhance their cybersecurity maturity by implementing governance and control measures appropriate to their individual level of risk. Regular security assessments and measuring posture against standards such as NIST or ISO27001 will ensure the business employs strong access controls, educates employees on cyber risks, updates software promptly, deploys advanced threat detection tools, and establishes an incident response plan. Regular training and the fostering of a digitally literate culture are crucial for an effective defence against cybercrime.

AP How can Triton help our companies with cybersecurity?

LA Triton operates a systematic cyber assessment and monitoring programme to help all portfolio companies protect their digital, physical, human resource and financial assets - Triton Cyber 360. This programme involves an initial assessment, a risk rating, and ongoing monitoring of cybersecurity maturity. The programme aims to help portfolio companies increase their cyber security maturity levels cost-effectively; protect and enhance the value of the business; and prevent business disruption, data loss, reputational damage and loss of contracts.

AP Companies can do a lot to control cybercrime risks within their direct corporate activities. But do they also face risks from activities involving their value chain partners?

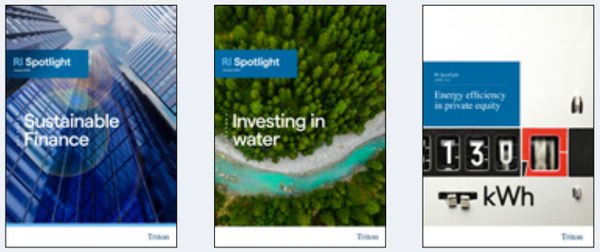
LA With the move to software-as-a-service platforms and cloud computing over the last decade, digital supply chain risk should be a focus area for all businesses who rely on these services for critical operations. Indeed, new regulations such as the EU's Digital Operational Resiliency Act (DORA), seek to ensure firms have sufficient protection against risks across their value chain partners.

AP Another topic saturating the news in 2023 was Artificial Intelligence. Does AI act as a cybercrime risk multiplier?

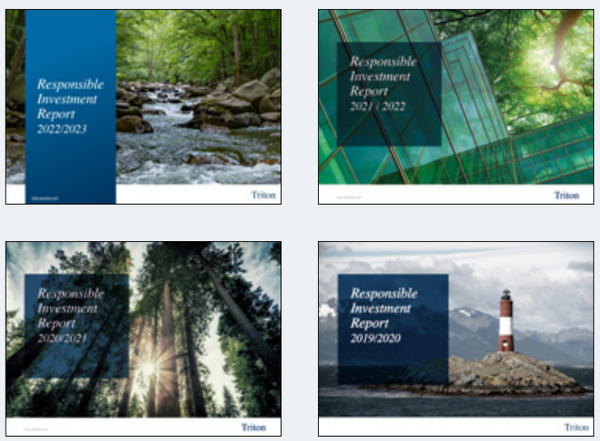
LA Cybercriminals have become increasingly sophisticated, organised, and motivated to capitalise on what has become a lucrative industry. The use of AI and generative AI, in particular, have given hackers a powerful new toolkit to deploy across all areas of cybercrime with increased velocity. Companies will need to employ new strategies and technical defences to counteract malicious use of AI technologies, such as "deepfake", which can manipulate digital content, typically in the form of images, videos, or audio recordings.

Triton Embedding cyber security - April 2024

Spotlights



Reponsible Investment reports



Disclaimer

The information contained in this Spotlight report (the 'Report') is made available by Triton Investment Management Limited (TIML) (together with its associates, 'Triton') for the sole purpose of providing certain information about Triton and funds, partnerships, other collective investment vehicles, managed account arrangement or separate accounts managed or advised by a Triton entity from time to time (together referred to as the 'Triton Funds'). In addition to the warnings, disclosures, and undertakings below, your attention is also drawn to any other rubrics or warnings provided on the face of any documents comprising the Information. This Report has not been approved by any supervisory authority and no regulatory approvals have been obtained in respect of the Report. Except as otherwise indicated herein, the information provided in the Report is based on matters as they exist as of the date of this Report and not as of any future date and may not be updated or otherwise revised to reflect information that subsequently becomes available, or circumstances existing or occurring after the date hereof. This Report is not, and under no circumstances is it to be construed as, a prospectus or an advertisement and the issuing of this Report is not, and under no circumstances is to be construed as, an offer to sell or a solicitation of an offer to purchase an interest in the Triton Funds. Recipients of this Report should not treat the contents of this Report as advice relating to legal, taxation, ERISA, financial, investment, business, or accounting matters, or as a recommendation by Triton and are strongly advised to consult their own professional advisors concerning the acquisition, holding, or disposal of interests in a Triton Fund and the suitability of the investment for such investor. Certain information (including certain forward-looking statements and economic and market information) has been obtained from published and non-published sources prepared by third parties, including Non-Triton Report Providers. In addition, certain information has been obtained from companies in which investments have been made by funds and entities affiliated with Triton. While such sources are believed to be reliable for the purposes used in the Information, none of Triton or any of the Triton Parties assumes any responsibility for the accuracy or completeness of such information, and such information has not been independently verified by Triton. All statements of opinion and/or belief contained in this Report and all views expressed and all discussion of past investment performance or decisions, projections, forecasts, or statements relating to expectations regarding future events represent Triton's own assessment and interpretation of information available to it as at the date of this Report and are subject to change without notice based on market and other developments. No representation is made, assurance given, or implication created that such statements, views, projections, track records or forecasts are correct after such date or that the objectives of Triton will be achieved. TIML is registered with the Jersey Financial Services Commission (the 'Commission') pursuant to the Financial Services (Jersey) Law 1998 (the 'FS Law') to provide fund services business as a manager. The Commission is protected by the FS Law against liability arising from the discharge of its functions under the FS Law. The approval of the Commission in respect of this Presentation is not required and has not been sought. In the United Kingdom this Report is also being distributed by Triton Investments Advisers LLP (TIA). TIA is a limited liability partnership incorporated pursuant to the Limited Liability Partnerships Act 2000 and having its registered office at 32 Duke Street, London SW1Y 6DF. TIA is authorised and regulated by the United Kingdom Financial Conduct Authority.

Europe

Triton Advisers (Finland) Oy

Ludviginkatu 3-5, (3 Floor)
00130 Helsinki
Finland

Triton Beratungsgesellschaft.

Große Gallusstraße 18
60312 Frankfurt am Main

Triton Advisers (Italy) Srl.

Via Maurizio Gonzaga 5
20123 Milan
Italy

Triton Investments Management Limited.

5/6 Esplanade, 1st Floor
St. Helier,
Jersey,
JE2 3QA

Triton Investments Management S.à r.l

Oksigen
Floor 7
2 rue Edward Steichen
L-2540 Luxembourg

Triton Advisers (Norway).

Kronprinsesse Märthas Plass 1
0160 Oslo
Norway

Triton Advisers Sweden

Kungsträdgårdsgatan 20,
7th floor
111 47 Stockholm

Triton Advisers (Netherlands) B.V.

ITO Toren Building M
Gustav Mahlerplein 28
1082 MA Amsterdam
The Netherlands

Triton Investments Advisers LLP

32 Duke Street, 3rd Floor
St James's
London
SW1Y 6DF

North America

Triton USA L.P.

300 Park Ave - Suite 1302
New York, NY 10022
United States

Asia

Triton Advisers (Shanghai) Co. Ltd

W18, 22/F, Tower 3
Jing An Kerry Center
1228 Yan An Zhong Road
Shanghai 200040, P.R China